

1 CLAIMS

2 What is claimed, is:

3 1. A data storage device for an information processing
4 device, the data storage device comprising:

5 an encryption circuit for encrypting desired data and
6 personal identification information by use of an encryption
7 key created out of a given piece of the personal identifica-
8 tion information;

9 a recording medium for recording the data and the
10 personal identification information encrypted by the encryp-
11 tion circuit; and

12 a control unit for executing user verification by use
13 of the encrypted personal identification information stored
14 in the recording medium.

15 2. The data storage device according to claim 1,

16 wherein the encryption circuit encrypts the encryption
17 key by use of a different encryption key, and

18 the recording medium records the encryption key
19 encrypted by use of the different encryption key.

20 3. The data storage device according to claim 1,

21 wherein the recording medium includes a special
22 storage area which is inaccessible in normal use, and

23 the recording medium records the encryption key in the
24 special storage area.

25 4. The data storage device according to claim 1,

1 wherein the encryption circuit creates a plurality of
2 encryption keys out of a plurality of personal identifica-
3 tion information and controls the user identification and
4 the data encryption depending on each of the plurality of
5 encryption keys, and

6 the recording medium manages the storage areas in
7 accordance with the plurality of keys, and records the
8 encrypted data in the respective storage areas by use of the
9 corresponding encryption keys.

10 5. A data storage device for an information processing
11 device, the data storage device comprising:

12 an encryption circuit for encrypting desired data by
13 use of a first encryption key and for encrypting the first
14 encryption key and personal identification information by
15 use of a second encryption key created out of a given piece
16 of the personal identification information;

17 a recording medium for recording the data encrypted by
18 use of the first encryption key, the first encryption key
19 encrypted by use of the second encryption key, and the
20 personal identification information encrypted by use of the
21 second key; and

22 a control unit for executing user verification by use
23 of the encrypted personal identification information stored
24 in the recording medium.

25 6. The data storage device according to claim 5,

26 wherein the encryption circuit decrypts the encrypted
27 first encryption key being read out of the recording medium
28 by use of the second encryption key, and executes any of
29 encryption and decryption of the desired data by use of the

1 decrypted first encryption key.

2 7. A hard disk device comprising:

3 a magnetic disk being a recording medium;

4 a read-and-write mechanism for writing and reading
5 data in and out of the magnetic disk; and

6 a control mechanism having an encryption function for
7 encrypting data to be written in the magnetic disk and for
8 decrypting the encrypted data to be read out of the magnetic
9 disk, the control mechanism for controlling reading and
10 writing the data by the reading-and-writing mechanism,
11 wherein the control mechanism executes encryption of
12 the data to be written in the magnetic disk for each unit of
13 writing and reading data in and out of a storage area of the
14 magnetic disk upon processing of writing the data in the
15 magnetic disk, in response to turning on and off of the
16 encryption mechanism.

17 8. The hard disk device according to claim 7,

18 wherein the control mechanism judges as to whether the
19 data are encrypted or not upon reading the data out of the
20 storage medium, and further decrypts the data when the data
21 are encrypted.

22 9. The hard disk device according to claim 7,

23 wherein the control mechanism decrypts the read-out
24 data when the data read out of the recording medium are
25 encrypted, and

26 the control mechanism encrypts and writes the data in
27 the recording medium when the encryption function is turned
28 on.

1 10. The hard disk device according to claim 7,
2 wherein the control mechanism includes an encryption
3 function for encrypting desired data and personal identifi-
4 cation information by use of an encryption key created out
5 of a given piece of the personal identification information,
6 and
7 the control mechanism executes user verification by
8 use of the encrypted personal identification information.

9 11. The hard disk device according to claim 10,
10 wherein the encryption function of the control mecha-
11 nism creates a plurality of encryption keys out of a plural-
12 ity of personal identification information and controls the
13 user identification and the data encryption depending on
14 each of the plurality of encryption keys, and
15 the magnetic disk manages storage areas in accordance
16 with the plurality of keys, and records the encrypted data
17 in the respective storage areas by use of the corresponding
18 encryption keys.

19 12. The hard disk device according to claim 7,
20 wherein the control mechanism includes an encryption
21 function for encrypting desired data by use of a first
22 encryption key and for encrypting the first encryption key
23 and personal identification information by use of a second
24 encryption key created out of a given piece of the personal
25 identification information, and

26 the control mechanism executes user verification by
27 use of the encrypted personal identification information.

28 13. An information processing device comprising:

1 an operation control unit for executing various opera-
2 tion processing; and
3 a data storage device for storing data to be processed
4 by the operation control unit,
5 wherein the data storage device includes an encryption
6 function for encrypting desired data by use of a data
7 encryption key and for encrypting personal identification
8 information by use of an verification encryption key created
9 out of a given piece of the personal identification informa-
10 tion, and
11 the data storage device executes user verification by
12 use of the encrypted personal identification information.

13 14. The information processing device according to claim
14 13, wherein the data encryption key and the verification
15 encryption are mutually identical.

16 15. The information processing device according to claim
17 13, wherein the data storage device encrypts the data
18 encryption key by use of a different encryption key and
19 saves the encrypted data encryption key.

20 16. The information processing device according to claim
21 15,
22 wherein the data storage device encrypts the data
23 encryption key by use of the verification encryption key as
24 the different encryption key.

25 17. A data processing method for a data storage device for
26 executing data writing and reading in and out of a recording
27 medium of a data storage device, the data processing method
28 for a data storage device comprising the steps of:

1 creating an encryption key out of a given piece of
2 personal identification information;
3 encrypting the personal identification information by
4 use of the encryption key and thereby recording the
5 encrypted personal identification information in the record-
6 ing medium as verification data;
7 executing user verification based on the verification
8 data recorded in the recording medium; and
9 executing any of encrypting write data transmitted
10 from a host system by use of the encryption key and thereby
11 recording the encrypted write data in the recording medium,
12 and, decrypting the data read out of the recording medium by
13 use of the encryption key and thereby transmitting the
14 decrypted data to the host system.

15 18. The data processing method for a data storage device
16 according to claim 17, further comprising the steps of:

17 encrypting the encryption key by use of a different
18 encryption key and thereby recording the encrypted encryp-
19 tion key in the recording medium; and

20 decrypting the encrypted encryption key by use of the
21 different encryption key and thereby decrypting the data
22 read out of the recording medium by use of the decrypted
23 encryption key.

24 19. A data processing method for a data storage device for
25 executing data writing and reading in and out of a recording
26 medium of a data storage device, the data processing method
27 for a data storage device comprising the steps of:

28 creating a verification encryption key out of a given
29 piece of personal identification information;

1 encrypting the personal identification information by
2 use of the verification encryption key and recording the
3 encrypted personal identification information in the record-
4 ing medium as verification data, and further encrypting a
5 data encryption key by use of the verification encryption
6 key and thereby recording the encrypted data encryption key
7 in the recording medium;
8 executing user verification based on the verification
9 data recorded in the recording medium;
10 decrypting the data encryption key recorded in the
11 recording medium by use of the verification encryption key;
12 and
13 executing any of encrypting write data transmitted
14 from a host system by use of the decrypted data encryption
15 key and thereby recording the encrypted write data in the
16 recording medium, and decrypting the data read out of the
17 recording medium by use of the data encryption key and
18 thereby transmitting the decrypted data to the host system.

19 20. The data processing method for a data storage device
20 according to claim 19, further comprising the step of:
21 decrypting the encrypted data encryption key recorded
22 in the recording medium along with a change in the personal
23 identification information by use of the verification
24 encryption key created out of the personal identification
25 information prior to the change, and then encrypting the
26 data encryption key again by use of the verification encryp-
27 tion key created out of the personal identification informa-
28 tion after the change and thereby storing the data
29 encryption key in the recording medium.

1 21. The data processing method for a data storage device
2 according to claim 19, further comprising the step of:
3 decrypting the encrypted data encryption key recorded
4 in the recording medium upon disabling encryption of the
5 data recorded in the recording medium by use of the verifi-
6 cation encryption key created out of the personal identifi-
7 cation information prior to a change and thereby storing the
8 decrypted data encryption key in the recording medium.

9 22. A program for controlling a computer to control data
10 writing and reading in and out of a magnetic disk, the
11 program causing the computer to execute the processes of:
12 creating an encryption key out of a given piece of
13 personal identification information;
14 encrypting the personal identification information by
15 use of the encryption key and thereby recording the
16 encrypted personal identification information in the
17 magnetic disk as verification data;
18 executing user verification based on the verification
19 data recorded in the magnetic disk; and
20 executing any of encrypting write data transmitted
21 from a host system by use of the encryption key and thereby
22 recording the encrypted write data in the magnetic disk, and
23 decrypting the data read out of the magnetic disk by use of
24 the encryption key and thereby transmitting the decrypted
25 data to the host system.

26 23. A program for controlling a computer to control data
27 writing and reading in and out of a magnetic disk, the
28 program causing the computer to execute the processes of:
29 creating an verification encryption key out of a given

1 piece of personal identification information;
2 encrypting the personal identification information by
3 use of the verification encryption key and recording the
4 encrypted personal identification information in the
5 magnetic disk as verification data, and further encrypting a
6 data encryption key by use of the verification encryption
7 key and thereby recording the encrypted data encryption key
8 in the magnetic disk;
9 executing user verification based on the verification
10 data recorded in the magnetic disk;
11 decrypting the data encryption key recorded in the
12 magnetic disk by use of the verification encryption key; and
13
14 executing any of encrypting write data transmitted
15 from a host system by use of the decrypted data encryption
16 key and thereby recording the encrypted write data in the
17 magnetic disk, and decrypting the data read out of the
18 magnetic disk by use of the data encryption key and thereby
19 transmitting the decrypted data to the host system.